

bsi.

You have 72 hours to respond after a breach... was personal data compromised?

Conor Gavin

Damir Kahvedžić

Senior eDiscovery & Forensics Consultants



**Through the passion and expertise
of our people, BSI embeds
excellence in organizations across
the globe to improve business
performance and resilience.**

Cybersecurity and Information Resilience – what we do

We enable organizations to secure information from cyber-threats, strengthening their information governance and in turn assuring resilience, mitigating risk whilst safeguarding them against vulnerabilities in their critical infrastructure.

bsi.



What do we do?



Cybersecurity

Penetration testing, vulnerability management, incident response and cloud security services.



Security awareness

Phishing and user awareness training, SaaS solutions, social engineering and simulation testing



Data management and privacy

GDPR services, information lifecycle management and eDiscovery and forensics

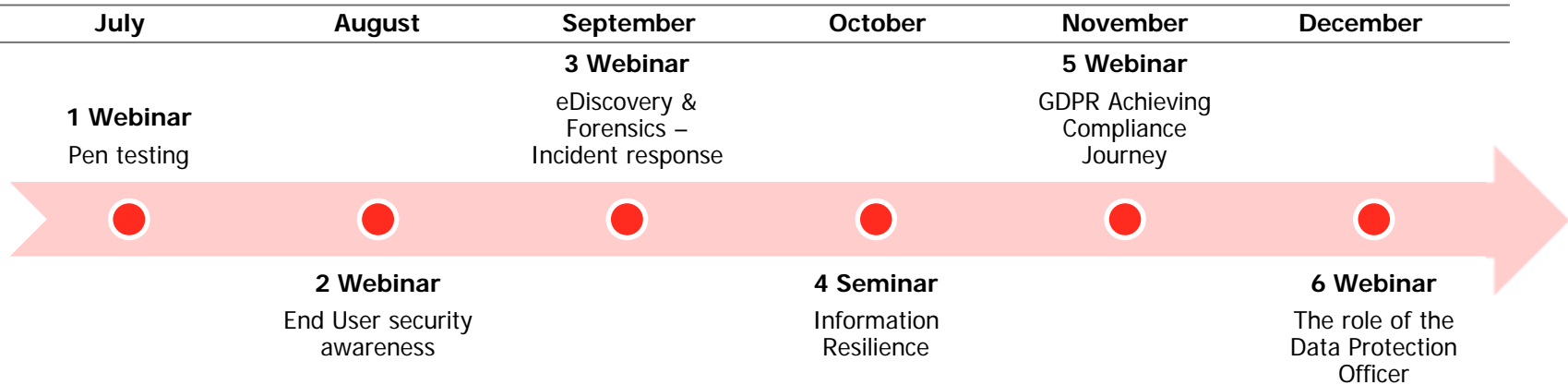


Compliance and testing

PCI DSS services, cyber lab testing and product and software assessments (CC, CAS-T/CPA)



Path to GDPR – Cybersecurity and Information Resilience Services



Webinar Series:

- 1. Penetration Testing (Jul17)** – ensuring an organization's customer and prospect data is secure
- 2. End User Security Awareness (Aug17)** – Untrained employees - the weakest link in your cybersecurity defence
- 3. Incident Response (Sept17)** – You have 72 hours to respond after a breach... was personal data compromised?
- 4. Information Resilience Series Event (Oct17)** – Manchester 17th October 2017
- 5. GDPR Achieving Compliance Journey (Nov17)** – a step-by-step methodology for achieving compliance
- 6. GDPR – the role of the Data Protection Officer (Dec17)** – Is your organization's DPO ready?

Understanding

Awareness and training courses

One day training course

We help you understand the fundamentals of GDPR

- Gain the confidence to interpret data protection regulations
- Learn to integrate GDPR policies and procedures
- End user security awareness training

Scoping workshop

Stakeholder engagement

We identify relevant information, activities and controls

- Compile inventories of Personally Identifiable Information (PII)
- Identify data flows and data processors
- Confirmation of regulatory requirements

Implementation

Gap analysis

Identify gaps in compliance

We assist you to identify the critical areas in need of improvement

- Gap analysis against GDPR requirements
- Verification assessment Audit against privacy standards (e.g. BS10012, ISO 29000)

Implementation support

Implement the key principles of GDPR

We help you establish the necessary policies and procedures

- Outsourced Data Protection Officer services
- Data breach reporting
- Privacy by design
- Completion of Baseline Privacy Impact Assessment (PIA)
- Project/change based PIAs

Validation

Ongoing support

Validation and response services

We offer a partner programme service for essential assistance

- Audits - internal, 3rd party/ supply chain
- Data breach/incident on-call support
- Subject access request support services
- Supervisory authority audit support

The Scenario

- You or your IT team get a call that you may have an incident. It seems that your IT systems have been breached.
- You don't know:
 - how it happened?
 - for how long did it go on?
 - who it affected in your company?
- Worse, you don't know what client data was affected
- You have 72 hours to respond... What do you do?



High Profile Breaches

You are not the only ones...



CENTRE SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

Security

Last year's ICO fines would be 79 times higher under GDPR

TalkTalk's £400,000 penalty was big – how about £59 MILLION?

By John Leyden 28 Apr 2017 at 08:03 29 SHARE



Equifax says 143 million hit in data breach

Credit reporting giant said "criminals" accessed data such as Social Security numbers and birth dates.

8 hours ago | Technology



Home Video World UK Business Tech Science Magazine Entertainment & Arts

Technology

AA Shop investigating 13 gigabyte data breach

3 July 2017 | Technology f t + e Share



SEARCH Cloud CXO Software Startups Innovation More Newsletters Forums Resource Library Tech Pro Free Trial

SECURITY

Yes, Yahoo's 1B data breach victims can sue the company, judge says

A US judge has ruled that users can sue Yahoo over a host of breaches that occurred between 2013 and 2016.

By Conner Forrest | September 5, 2017, 8:12 AM PST

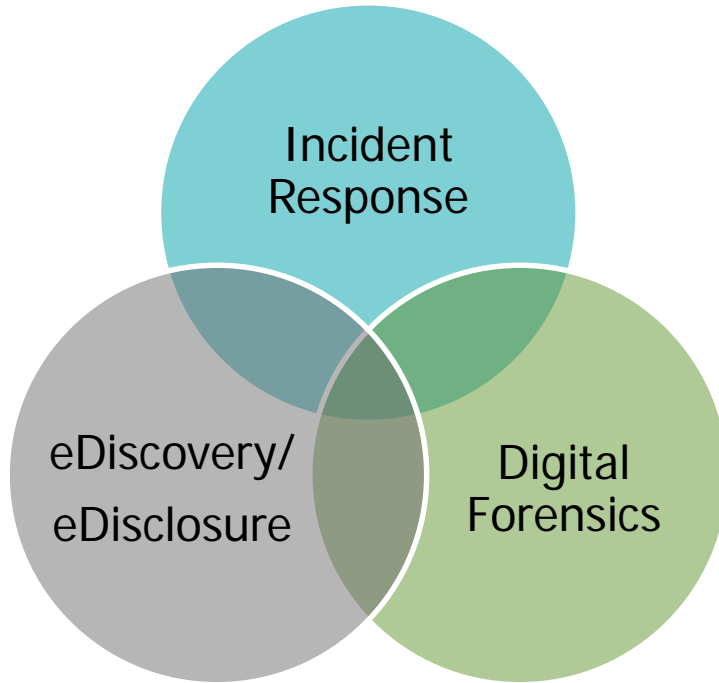


Markets Tech Pursuits Politics Opinion Businessweek Subscribe to B

Sweden Tries to Stem Fallout of Security Breach in IBM Contract

By Niklas Magnusson and Niklas Rolandar
July 24, 2017, 5:54 PM GMT+1 | Updated on July 24, 2017, 11:00 PM GMT+1

Overlap of Disciplines



Focus is usually to address and mitigate the immediate impact of the breach to the business

But what about the impact to the public?

General Data Protection Regulation in 1 Minute

- Aims to **protect** the personal data of EU citizens
- Puts individuals back in **control** of their personal data
- Applies to all EU member states, any organization who operates within the EU market, or who holds information on EU data subjects
- Requirement to **report** a data breach to the data protection commissioner, within 72 hours of becoming aware of any breach
- **Fines** of up to €20 million or up to 4% of annual worldwide turnover for non-compliance
- Comes into force on the **25th May 2018**
- Data Protection Officer (DPO) appointment **mandatory**
- No opt out for UK with **Brexit**



What is the definition of an incident?

“**Data Breach incident**” means any real or suspected event that may involve the loss or disclosure of personal or sensitive personal data.

Examples include:

- Unauthorized access to data, especially confidential data like a person’s name and address
- Loss of a device which includes personal information
- Security breach incident where personal data may have been accessed
- Verbal disclosure to an unauthorised party
- Email with personal information being sent to the wrong destination
- etc.

Incident Response & Breach Reporting

- Data controllers must notify most data breaches to the **Data Protection Authority** (DPA)
- “Where feasible” **no later than 72 hours** after the breach
- A **reasoned** justification must be provided if this timeframe is not met
- Where there is a **high risk** to the data subject due to the breach, they must also be notified “without undue delay”

Incident Response & Breach Reporting

Exemptions:

- Notification does not need to be made to the DPA if the breach is unlikely to result in a risk to the rights and freedoms of individuals
- The threshold for notification to data subjects is that there is likely to be a “high risk” to their rights and freedoms
- So for example, if encryption has been applied, no risk presents itself

Incident Response & Breach Reporting

What does a notification look like?

- Notification must include:
 - Categories and approximate numbers of individuals and records concerned
 - The name of the organisation's Data Protection Officer
 - Consequences of the breach
 - Measures to mitigate the harm

Your responsibilities after an attack

Identification of the lost data is key.

This lost data will need to have its contents analysed.

The main question to ask:

- Is there any **Personally Identifiable Information** in the lost data?

What is the definition of **PII**?

Definition of PII







"Personal data" means:

data relating to a living individual who is or can be identified either:

- i. from the data, or
- ii. from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Poll 2 Discussion

Will the following be considered personal data?

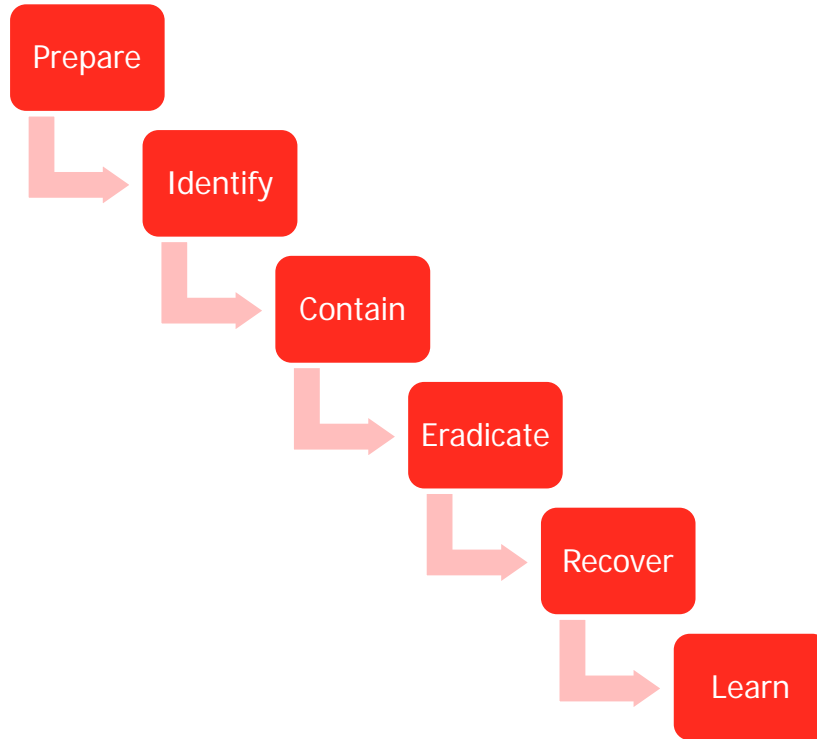
- Credit card number? 
- Telephone number? 
- IP address? 
- Location data? 
- Employee ID?  

Incident Response & Breach Reporting

- But how do we classify the incident?
- How can we evaluate the incident and identify the people and data involved quickly?



6 Stages of Incident Response



Case Study 1

- Spear phishing attack to key users
- Some are known to have clicked the link
- Credentials stolen
- Intruder:
 - Setup an account for himself
 - Setup auto-forwarding rules on key personnel
 - Received a copy of every mails for 6 months
- What has been taken?
- Who needs to be notified?



Case Study 1 - Response

- Gather logs
 - Examine emails \ email settings
 - Confirm that the incident is valid and that the suspicions were correct
- Cross-correlate:
 - Examine the emails for the phishing links
 - Search web proxy logs for users who clicked the link
 - For all identified users, examine their mailbox logs
- Eradicate
 - Was any ongoing damage done by the intruder?
- Recover
 - Password reset for users
 - 2-factor authentication implemented
 - **Identify if it was a GDPR data breach**



Identify



Contain



Eradicate



Recover

Case Study 2

Online Web Shop Breach

- FTP Server compromised
- BSI examined the FTP logs
- Found evidence of a malicious IP connecting and downloading data
- Data downloaded contained shipping information about end customers
 - Customer Name
 - Home Address
 - Email Address
 - Phone Number



Case Study 2

- BSI's analysis was able to identify:
 - Details of the quantity and nature of the stolen data
 - Number of unique individuals that were contained in that dataset
 - Country of residence of each individual
 - Reason why the server was compromised

Identify

Contain

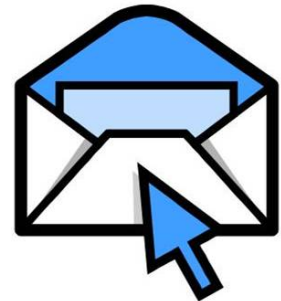


Case Study 2

- This allowed the client to:
 - Fix the underlying issue on the compromised server
 - Contact each individual to notify them of the breach
 - Inform the DPA in each affected country of the data breach
 - Tailor their notification to the DPA in each country based on applicable local laws
 - Demonstrate that a thorough investigation had taken place

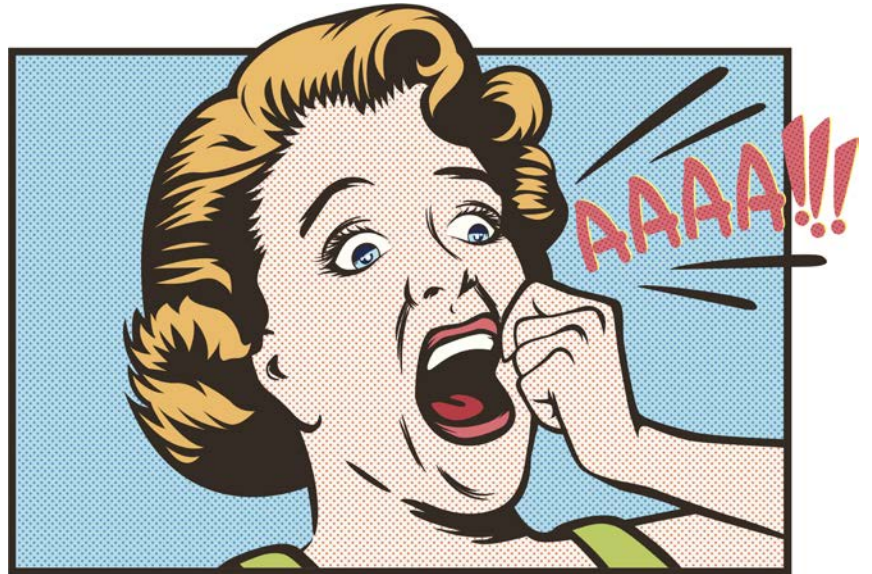
Eradicate

Recover



The nightmare scenario

- Evidence has been found of massive amounts of data being
 - Lost
 - Stolen
 - Downloaded
 - Forwarded
- What is in the data?
- What did the intruder take?

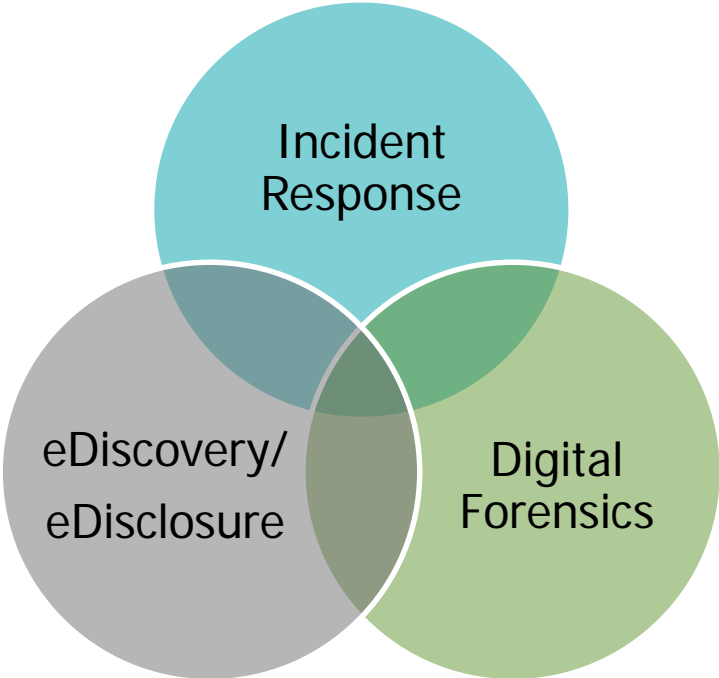


Analysis of Breached Data

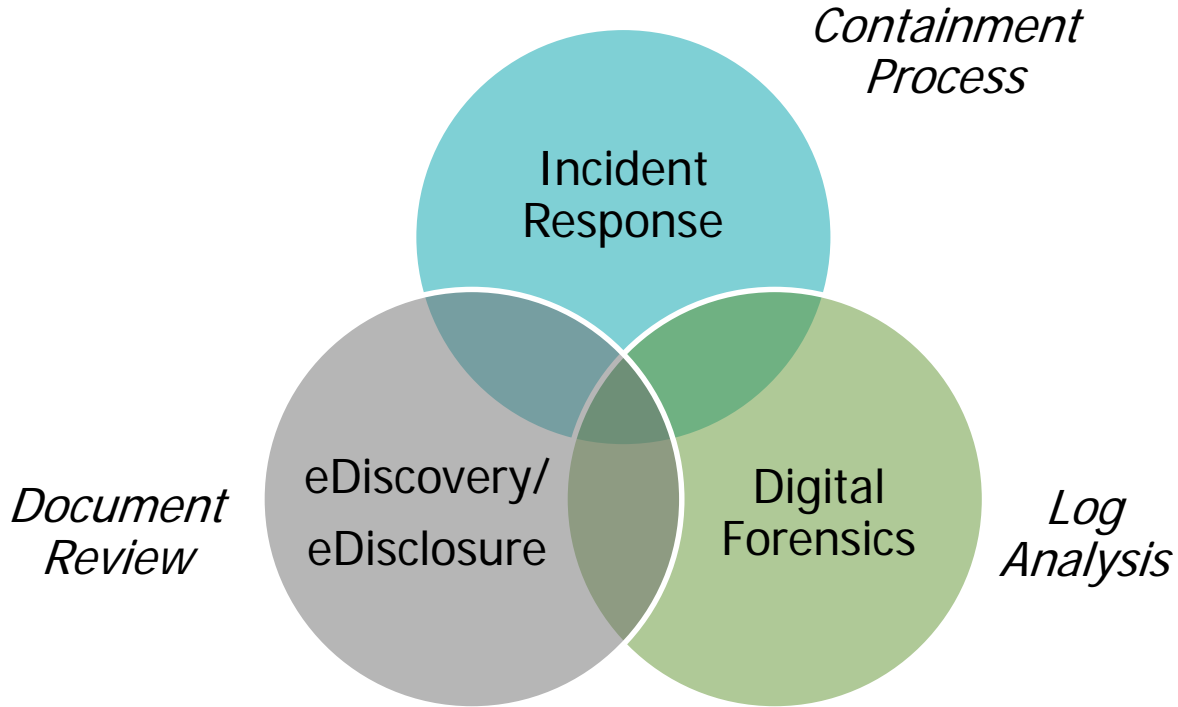
- For many types of breaches, it can be difficult to identify the content of the data
- Email breach – mails forwarded to third party
 - What was recently sent or received?
 - What logs are available?
 - What was in the mailbox?
 - Ask yourself: How many emails have you received in the last 6 months?
- **Case Study 1: How can we analyse 100,000 emails for PII?**
- **Case Study 2: How can we analyse millions of log entries from the fileserver for evidence of PII being stolen?**



Overlap of Disciplines



Overlap of Disciplines




Overlap of Disciplines

- Traditionally used in response to litigation
- Obligation to provide relevant material to court
- Large scale document reviews undertaken

New uses:

- Identification and classification of PII
- Responding to Subject Access Requests (SAR)



eDiscovery/
eDisclosure

Overlap of Disciplines

- Digital forensics skills key to understanding what data was taken
- Some breaches more straightforward
 - e.g. compromise of cloud system credentials like Office 365
- “Roving” attacker more complicated
 - Attacker is inside the network and moves from system to system
 - Can require analysis of multiple machines and workstations
- How good are your logs?
 - Mailbox auditing?
 - Server and workstation logon events?
 - File share access?



Digital
Forensics

Software Profile

Nuix Investigator Workstation

- Can process large volumes of data quickly
- Keyword search data
- Classify information such as names, email address, phone numbers, credit card information
- Log analysis

Nuix Investigator Workstation

The image displays the Nuix Investigator Workstation interface, showing search results, analysis graph, and analysis table.

Search Results: The search criteria are "(named-entities:"money":250,ADUSD" OR "money:5m USD")". The results show 4 evidence items (32,669 hits, 0.01%). The filtered items include:

- labbetaABC (4)
- labbetaABC (1)
- labbetaABC (7)
- labbetaABC (3)

Analysis Graph: A circular graph showing relationships between entities. The graph includes nodes for "labbetaABC", "money", "ADUSD", "5m USD", and "money:5m USD". The graph also shows relationships between "labbetaABC" and "money", "ADUSD", "5m USD", and "money:5m USD".

Analysis Table:

Date	Date Type	Name	File Type	Item Date	Cookie/Host
Friday, 19 June 2015 at 14:33:...	Skype created_timestamp	[money:mam79@skype, diamond.geezer94@skype]	Skype Chat Convers...	Sunday, 21 June 2015 at 22:59:50 British Summer Time	
Friday, 19 June 2015 at 14:35:...	Item Date	2015-06-19 13:35:23 UTC: diamond.geezer94@skype -> [money:mam79@skype]	Skype Chat Message	Friday, 19 June 2015 at 14:35:23 British Summer Time	
Friday, 19 June 2015 at 14:43:...	Item Date	2015-06-19 12:43:40 UTC: diamond.geezer94@skype -> [money:mam79@skype]	Skype Chat Message	Friday, 19 June 2015 at 14:43:40 British Summer Time	
Friday, 19 June 2015 at 14:47:...	Skype inbound_timestamp	[money:mam79@skype, diamond.geezer94@skype]	Skype Chat Convers...	Sunday, 21 June 2015 at 22:59:50 British Summer Time	
Friday, 19 June 2015 at 14:47:...	Skype meta_active_timestamp	[money:mam79@skype, diamond.geezer94@skype]	Skype Chat Convers...	Sunday, 21 June 2015 at 22:59:50 British Summer Time	
Friday, 19 June 2015 at 19:52:...	Item Date	D76348582023446E94B70D243A9480E60DASCA.FileSlick	Unknown Binary File	Friday, 19 June 2015 at 19:52:26 British Summer Time	
Sunday, 21 June 2015 at 22:59:...	Skype history_horizon	[money:mam79@skype, diamond.geezer94@skype]	Skype Chat Convers...	Sunday, 21 June 2015 at 22:59:50 British Summer Time	

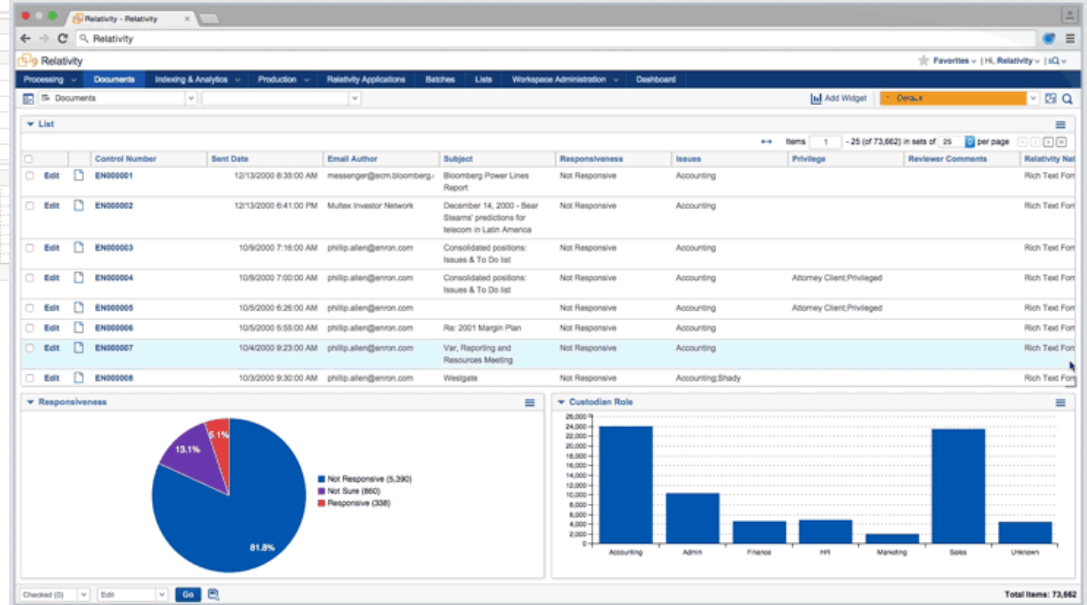
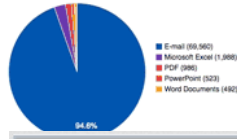
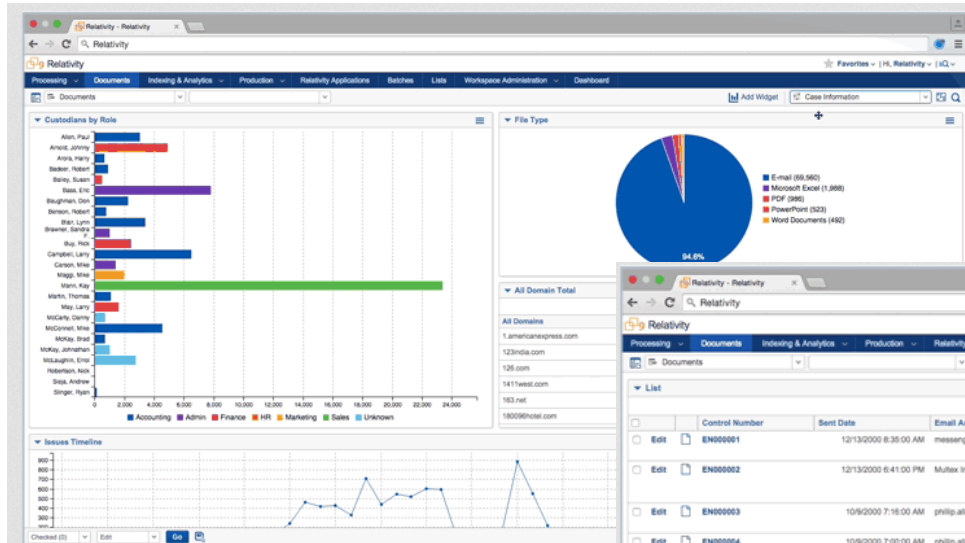
Displaying 7 events, 4 items shown.

Software Profile

Relativity

- Large scale review platform
- Ideal for multiple users to review simultaneously
- Powerful analytics
- Redaction capabilities

Relativity



BSI

BSI utilises these software and others to interrogate the data associated with the breach

Evidence from multiple sources and logs are correlated and interpreted together to get to the root of the matter quickly

We can help you identify and PII in your data and advise on the best course of action to:

- Recover from the breach
- Remediate the threat for the future
- Comply with GDPR and other regulations

BSI can tailor solutions to businesses of all sizes and capabilities

The Bad News

No one element will solve your problems

For a large breach, you may need...

- Digital forensics experts
- Data review capability
- Specialist software
- Experience
- Legal advice



The Good News

BSI Cybersecurity and Information Resilience consultants provide:

- Digital forensics expertise ✓
- Data review capability ✓
- Specialist software ✓
- Experience ✓
- ~~Legal~~ Expert advice ✓



Understanding

Understand your responsibilities

Understand your capabilities

Understand the limitations of the logs of 3rd party providers

Implementation

Prepare for the worst!

Know where your information is

Implement IR procedures

Validation

Contact experts

Get in touch

UK – Incident Response

Phone: 00 44 345 222 1711

Email: cyber@bsigroup.com

Global – Incident Response

Phone: 00 353 1 210 1711

Email: cyber.ie@bsigroup.com